August 5, 2014

Sent via Email to privacyrfc2014@ntia.doc.gov

Mr. John Morris, Associate Administrator
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Re: Request for Public Comment on ‘‘Big Data’’ Developments and How They Impact the Consumer Privacy Bill of Rights - Docket No. 140514424–4424–01

Dear Mr. Morris,

Pursuant to the request for public comments issued by the National Telecommunications & Information Administration (“NTIA”) published in the Federal Register at 79 Fed. Reg. 32,714 (“NTIA Request For Public Comments”), Anonos respectfully submits this Comment Letter with specific responses to questions 1, 4, 7, 11, and 13 through 17 of the NTIA Request For Public Comments.

Introduction

As technology capabilities expand, the ability to process and analyze large complex data sets offers an unprecedented opportunity to address the critical health, security, scientific, commercial and economic issues facing our nation.[1] Whether it is aggregating data to study correlations in disease, ensuring our nation is safe from cyber-attack, or optimizing business efficiency, *big data has a role to play in keeping America competitive.*

Although these technological advances provide significant promise, data breaches and the unauthorized use of personal information by government and industry are eroding confidence that personal data will be used in appropriate and responsible ways. It is critical to ensure that consumers and citizens trust that their data is private and protected. *Without a foundation of*

[1] President’s Council of Advisors on Science and Technology (PCAST), Report to the President; *Big Data and Privacy: A Technological Perspective*, Section 2. Examples and Scenarios (May 2014). Available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big _ data_and_privacy_-_may_2014.pdf.

trust, businesses, government, and researchers will be unable to realize the full potential and societal benefits of big data capabilities.

Responses to NTIA Request For Public Comments Questions

1. How can the Consumer Privacy Bill of Rights, which is based on the Fair Information Practice Principles, support the innovations of big data while at the same time responding to its risks?

We believe innovations of big data can be supported while at the same time managing associated risks by increasing participation by the private sector in developing tools that provide consumers with *greater transparency and control at the data element level as necessitated by the realities of big data*. The Consumer Privacy Bill of Rights[2] expressly acknowledges the importance of private sector participation in achieving its goals and objectives via statements like those found on page 12, "Innovative technology can help to expand the range of user control," and page 15, "This level of transparency may also facilitate the development within the private sector of innovative privacy-enhancing technologies and guidance that consumers can use to protect their privacy."

Exhibit 1 to this Comment Letter provides an overview of the Anonos private sector Dynamic Anonymity[3] risk management platform. *More importantly than what Anonos represents in its own right, is what it represents as a category – private sector developed privacy-enhancing technologies*. Private sector developed privacy-enhancing technologies can help to reconcile tensions between identifiable and functional information by providing tools that enable trust and control in order to achieve the goals and objectives of the Consumer Privacy Bill of Rights. However, as evidence of the general failure of the private sector to step up to this challenge, as recently as October 2013, FTC Commissioner Julie Brill exhorted the audience at the Polytechnic Institute of New York University (NYU-Poly) Third Sloan Foundation Cyber Security Lecture, by stating "And you -- the engineers, computer scientists, and technologists -- you can help industry develop this robust system for consumers….This is your 'call to arms'--or perhaps, given who you are, your 'call to keyboard' -- to help create technological solutions to some of the most vexing privacy problems presented by big data."[4]

[2] Available at http://www.whitehouse.gov/sites/default/files/privacyfinal.pdf
[3] Anonos, CoT, DDID, Dynamic Anonymity, and Dynamic De-Identifier are trademarks of Anonos.
[4] See http://engineering.nyu.edu/news/2013/11/05/ftc-commissioner-brill-warns-about-cyberspace-big-data-abuse

4. What mechanisms should be used to address the practical limits to the ''notice and consent'' model noted in the Big Data Report? How can the Consumer Privacy Bill of Rights' ''individual control'' and ''respect for context'' principles be applied to big data? Should they be? How is the notice and consent model impacted by recent advances concerning ''just in time'' notices?

The notice and consent model has been widely criticized as ineffective. In too many cases, particularly where electronic consent is obtained, a user clicks an "I Agree" button, perhaps after quickly scrolling through a consent form. This system does not build trust between individuals and the entities that use their data. As stated in the PCAST Report, "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent." [5] A lack of real consent erodes the trust between data owners and data users. And, while more detailed requirements for "just in time" notices have been a step in the right direction, it is still a stretch of the imagination to say consumer consent is knowingly and voluntarily provided when withholding consent prevents a consumer from using the application in question.

This current framework does not build trust with the individual and does not effectively serve researchers, business, or government. We see it in the news every day: the proliferation of technology, while opening some doors, has seemingly pitted privacy interests against the interests of national security and economic growth. Alternatives are needed that can help realize the promise big data holds and maintain the trust of consumers and citizens.

Privacy-enhancing technologies go by different names including "privacy-preserving technologies" and even "privacy substitutes" [6] but they all generally share the common goal of balancing functionality and protecting consumer privacy. When a more robust methodology that identifies data, retains utility, and provides individuals and trusted parties / proxies with the ability to manage access to personal data is needed, dynamic functional data obscurity provides a new and effective alternative.

Functional data obscurity is a new method to dynamically de-identify data while retaining its utility. Instead of stripping the identifying information from the data, which significantly reduces its value, functional data obscurity replaces the identifying information with obscure values that dynamically mask identity but preserve association. In this way, data privacy is protected, but analysis between data points is preserved.

[5] PCAST Report, at xi.
[6] Mayer, Jonathan & Narayanan, Arvind, *Privacy Substitutes*, 66 Stan. L. Rev. Online 89 (2013). Available at http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-substitutes

Functional data obscurity can apply the Consumer Privacy Bill of Rights' ''individual control'' and ''respect for context'' principles to big data in the following ways:

- When functional data obscurity is used, the utility of each data element is preserved and protected;
- Users get only the information they need and are entitled to receive - data subjects know their information is protected and limited; and
- Functional data obscurity fundamentally changes the way we treat data by providing individuals with different ways to assemble and access information.

The approach to functional data obscurity embodied in the Anonos Dynamic Anonymity risk management platform allows data subjects / trusted parties / proxies to determine on a time, place, and purpose-specific basis what data elements to share and what level of identifying information to include at the time of sharing. In addition, it enables *controlled data fusion* by providing controlled anonymity for data, identity of data subjects / trusted parties / proxies as well as "context" (e.g., time, purpose, place) by obfuscating connections between and among the foregoing, enabling the:

- Undoing or reversal of either rights granted or access to data; and
- Rejuvenation of data to support additional secondary uses without violating promises to data subjects.

The identifiers used by the Anonos Dynamic Anonymity risk management platform in providing functional data obscurity can be replaced dynamically at the data element level, not just at the data subject or data record level. This means that individual consumers and citizens can have control over what data is shared or accessed enabling effective dynamic de-identification without de-valuation. An individual no longer has to choose to share the entirety of their personal information or strip it of all its identifiers; instead, the individual (or a trusted party or proxy) can decide which elements to share with whom.

7. The PCAST Report states that in some cases ''it is practically impossible'' with any high degree of assurance for data holders to identify and delete ''all the data about an individual'' particularly in light of the distributed and redundant nature of data storage. Do such challenges pose privacy risks? How significant are the privacy risks, and how might such challenges be addressed? Are there particular policy or technical solutions that would be useful to consider? Would concepts of ''reasonableness'' be useful in addressing data deletion?

EMC and International Data Corporation estimate that the size of the digital universe doubles every two years, ever expanding to include an increasing number of people, enterprises and

smart devices connected to the Internet. They estimate that by 2020, the digital universe will contain nearly as many digital bits as there are stars in the universe and that the data we create annually will reach 44 zettabytes, or 44 trillion gigabytes.[7] In their law review article, *Big Data Ethics*, Neil Richards and Jonathan King explain how "…we as a society have effectively built a 'big metadata computer' that is now computing data and associated metadata about everything we do at an ever quickening pace. As the data about everything (including us) have grown, so too have big data analytics—new capabilities enable new kinds of data analysis and motivate increased data collection and the sharing of data for secondary uses."[8]

Richards and King go on to note that "Much of the tension in privacy law over the past few decades has come from the simplistic idea that privacy is a binary, on-or-off state, and that once information is shared and consent given, it can no longer be private. Binary notions of privacy are particularly dangerous and can erode trust in our era of big data and metadata, in which private information is necessarily shared by design in order to be useful."[9] While it may be "practicably impossible" to delete all the digital data information that has been amassed to date, privacy-enhancing technologies that can effectively de-identify without de-valuing data going forward enable us to benefit from the capabilities of big data while simultaneously managing risks.

The capabilities of privacy-enhancing technologies to de-identify without de-valuing data should be used to define what is "reasonable" going forward. They should be leveraged to:

- Significantly decrease risks associated with data breaches, misuse of personal data and re-identification;
- Maximize data use for businesses and government entities;
- Improve business models;
- Facilitate research and development; and
- Work within the current system to balance trust, control and utility.

This century has brought an explosion of data as well as the ability to make use of unstructured data. We can now make use of not just formalized data records but also data down to the data element level – and we can go even beyond the data element level to the "meta data level" – i.e., data related to data. We believe this is the real revolution in big data – not the volume of data but the diversity of data arising from the availability of meta data and unstructured data.

To really protect against potential abuses of big data, you need to be able to get down to the data element level so that organizations can be in control and, where possible and desired,

[7] EMC Digital Universe with Research & Analysis by IDC, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*. Available at http://www.emc.com/leadership/digital-universe/2014iview/index.htm.
[8] Richards, Neil and King, Jonathan, *Big Data Ethics* (2014) at 395. Wake Forest Law Review. Available at http://ssrn.com/abstract=2384174
[9] Id at 396.

extend controls to individuals. Control down to the data element level makes risk mitigation possible in the age of big data – beyond the reach of controls targeted only at the data record or data subject level. Ultimately, this creates capabilities that favor the Consumer Privacy Bill of Rights and enables tool kits that allow consumers to exercise more control.

11. As the PCAST Report explains, ''it is increasingly easy to defeat [deidentification of personal data] by the very techniques that are being developed for many legitimate applications of big data.'' However, deidentification may remain useful as an added safeguard in some contexts, particularly when employed in combination with policy safeguards. How significant are the privacy risks posed by re-identification of deidentified data? How can deidentification be used to mitigate privacy risks in light of the analytical capabilities of big data? Can particular policy safeguards bolster the effectiveness of deidentification? Does the relative efficacy of deidentification depend on whether it is applied to public or private data sets? Can differential privacy mitigate risks in some cases? What steps could the government or private sector take to expand the capabilities and practical application of these techniques?

With the ever-increasing amount of data being deposited into the "big metadata computer" we're building as a society,[10] there are ever-increasing risks of re-identification when static approaches to anonymity or de-identification are used. At least as early as 2000, experts like Latanya Sweeney, former Chief Technologist at the FTC, noted in her Carnegie Mellon University paper, *Simple Demographics Often Identify People Uniquely*,[11] the weakness of static identifiers in providing effective anonymity. Professor Paul Ohm, in his seminal 2009 article, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* revealed how computer scientists can re-identity individuals presumably hidden by statically anonymized data.[12] More recently, James Turow noted in his 2013 book, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*,[13] that this is particularly the case "when firms intermittently add offline information to online data and then simply strip the name and address to make it 'anonymous.'" However, continued private sector development of dynamic de-identification and Functional Data Obscurity capabilities such as embodied in the Anonos Dynamic Anonymity risk management platform described in Exhibit 1, particularly when employed in combination with policy safeguards, can mitigate re-identification privacy risks notwithstanding the analytical capabilities of big data and regardless of whether applied to public and / or private data sets.

---

[10] See notes 6 and 7, *supra*.
[11] Sweeney, Latanya, *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Available at http://dataprivacylab.org/projects/identifiability/.
[12] Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at http://ssrn.com/abstract=1450006.
[13] Turow, James, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*, Yale Press (2013). Available at http://yalepress.yale.edu/yupbooks/book.asp?isbn=9780300165012

13. Can accountability mechanisms play a useful role in promoting socially beneficial uses of big data while safeguarding privacy? Should ethics boards, privacy advisory committees, consumer advisory boards, or Institutional Review Boards (IRBs) be consulted when practical limits frustrate transparency and individuals' control over their personal information? How could such entities be structured? How might they be useful in the commercial context? Can privacy impact assessments and third-party audits complement the work of such entities? What kinds of parameters would be valuable for different kinds of big data analysts to consider, and what kinds of incentives might be most effective in promoting their consideration?

De-identification or anonymization is not about the perfection of technologies – making it impossible for data to ever be re-identified. Given enough time and the capabilities of supercomputers, one could argue that there is nothing that cannot eventually be re-identified. Rather, effective de-identification and anonymization are about limiting purpose and use to parties that a data subject has specifically authorized and sufficiently increasing the difficulty of third parties to gain access to, or misuse, personal information. You cannot just depend on technology – it has to be a blend of advanced technology and policies that go with it.

Even the most advanced toolsets may still be dependent in most cases on policy decisions. Technology does not have to be perfect – but it does need to be much better than what has been previously available. Advanced privacy-enhancing technology like the Anonos Dynamic Anonymity risk management platform make it possible to have access to tools to ensure that proper controls are available when data is used for different purposes.

Accountability requires policies and contracts as well as more effective tools that can bring control down to the data element level from the data record or data subject level. Effective privacy governance requires having access to more effective tools to recalibrate the equilibrium point via mitigation strategies. Once you understand the balancing points, you must have controls down to the data element level to achieve mitigation strategies – it is no longer "good enough" to have controls just at the data record or data subject level.

Ethics boards, privacy advisory committees, consumer advisory boards, and / or Institutional Review Boards (IRBs) can serve a valuable role in helping to determine the kind of tools, policies and contracts that represent "best practice."

14. Would a system using ''privacy preference profiles,'' as discussed in Section 4.5.1 of the PCAST Report, mitigate privacy risks regarding big data analysis?

We believe that "privacy preference profiles" along the lines discussed in Section 4.5.1 of the PCAST Report can play a role in mitigating privacy risks of big data analysis. However, we do not

necessarily agree with the statement in the PCAST report that "…the responsibility for using personal data in accordance with the user's preferences should rest with the provider, possibly assisted by a mutually accepted intermediary, rather than with the user."[14] As reflected in the discussion of the Anonos Circle of Trust (CoT) provided in Exhibit 1, *both data subject and data stewardship implementations* of privacy-enhancing technologies like the Anonos Dynamic Anonymity risk management platform are technically feasible. The goal of privacy-enhancing technologies should be to provide risk management / mitigation tools that can be used as determined appropriate by jurisdictionally empowered legislators and regulators – which in different situations may or may not include users having the ability to directly control use of data in accordance with personal privacy preference profiles.[15]

15. Related to the concept of "privacy preference profiles," some have urged that privacy preferences could be attached to and travel with personal data (in the form of metadata), thereby enabling recipients of data to know how to handle the data. Could such an approach mitigate privacy risks regarding big data analysis?

While "privacy preference profiles" attached as metadata could help identify sources of data breaches and misuse of personal data, they would only provide after-the-fact means of determining fault to assess culpability and award monetary damages. Our belief is that reputational damage is not always capable of being made entirely whole by means of monetary damages. A more effective means of honoring privacy preferences is to use them to establish allowable operations such as what data can be used by whom, for what purpose, what time period, etc. along the lines discussed on page 14 of Exhibit 1 in the context of "Permissions" or "PERMs" used by the Anonos Dynamic Anonymity risk management platform to specify desired anonymization levels and when / where / how to use Dynamic De-Identifiers (DDIDs) in the context of providing anonymity for the identity and / or activities of a data subject, when to use other privacy-enhancing techniques in connection with, or in lieu of, DDIDs, when to provide identifying information to facilitate transactions, etc.

16. Would the development of a framework for privacy risk management be an effective mechanism for addressing challenges with big data?

We strongly believe that privacy risk management frameworks are some of the most effective mechanisms for addressing many of the challenges with big data. Anonos was founded to leverage our knowledge and experience in previously successfully implementing financial

[14] PCAST Report at page 40.

[15] Providing users with the ability to directly control use of data in accordance with personal privacy preference profiles may be useful in helping to reconcile differences between EU "fundamental right" and US balancing of privacy rights / right to free expression / commerce perspectives on data privacy protection. For background, see American Bar Association Antitrust magazine article entitled "*So Close Yet So Far, The EU and US Visions of a New Privacy Framework*" by Hogan Lovells partners Winston Maxwell (Paris) and Chris Wolf (Washington) at *Antitrust*, Vol.26, No.3, Summer 2012; available at http://www.hldataprotection.com/uploads/file/ABA%20Antitrust%20Magazine(1).pdf.

securities risk management across the globe. As more fully described in Exhibit 1, before being acquired by NASDAQ OMX in 2010, our prior company, FTEN, was the largest processor of real-time financial securities risk management in the world – each trading day providing real-time risk management and surveillance for up to 17 billion executed shares of U.S. equities, accounting for $150 billion in risk calculations.[16] At Anonos, we are now applying this knowledge and experience to the data privacy sector to reduce the risk of inadvertent or unauthorized disclosure of identifying information.

Rather than offering control just at the data subject or data record level – which is primarily what Notice and Consent is about – the Anonos Dynamic Anonymity risk management platform can provide data privacy risk management tools down to the data element level. Tools that enable a relationship of trust and control can support risk mitigation by analyzing pros and cons of different types of transactions and helping to determine whether to permit them or not. Privacy-enhancing technology such as the Anonos Dynamic Anonymity risk management platform allow flexible, granular control – something previously not available.

17. Can emerging privacy-enhancing technologies mitigate privacy risks to individuals while preserving the benefits of robust aggregate data sets?

For the reasons outlined above and discussed in Exhibit 1, we believe privacy-enhancing technologies like the Anonos Dynamic Anonymity risk management platform can help mitigate privacy risks to individuals while preserving the benefits of robust aggregate data sets.

Anonos appreciates the opportunity to submit this Comment Letter in response to the NTIA's Request for Public Comment on ‘‘Big Data’’ Developments and How They Impact the Consumer Privacy Bill of Rights (Docket No. 140514424–4424–01).

Respectfully Submitted,

M. Gary LaFever
Co-Founder

Ted Myerson
Co-Founder

[16] See http://ir.nasdaqomx.com/releasedetail.cfm?ReleaseID=537252.

ANONOS ACKNOWLEDGES THAT THIS MATERIAL MAY BECOME PART OF THE PUBLIC RECORD AND POSTED TO HTTP://WWW.NTIA.DOC.GOV/CATEGORY/INTERNET-POLICY-TASK-FORCE. THIS INFORMATION DOES NOT CONSTITUTE CONFIDENTIAL BUSINESS INFORMATION BUT IS PROTECTED UNDER PATENT APPLICATIONS, INCLUDING BUT NOT LIMITED TO, U.S. APPLICATION NOS. 13/764,773; 61/675,815; 61/832,087; 61/899,096; 61/938,631; 61/941,242; 61/944,565; 61/945,821; 61/948,575; 61/969,194; 61/974,442; 61/988,373; 61/ 992,441; 61/994,076; 61/994,715; 61/994,721; 62/001,127; 14/298,723; 62/015,431; 62/019,987 AND INTERNATIONAL APPLICATION NO. PCT US13/52159. ANONOS, COT, DDID, DYNAMIC ANONYMITY, AND DYNAMIC DE-IDENTIFIER ARE TRADEMARKS OF ANONOS.

Exhibit 1

Introduction to the Anonos Dynamic Anonymity Risk Management Platform

The Anonos Dynamic Anonymity risk management platform currently under development is designed to provide the benefit of minimizing risk of identity disclosure while respecting and protecting digital rights management for individuals / trusted parties / proxies – enabling them, at their election and control, to avail themselves of the benefits of big data.

Risk Management by Associating Unassociated Data Elements – the Financial Industry

In 2003 at their prior company, FTEN, the founders of Anonos helped develop technology that utilized real-time electronic "drop copies" of data from trading venues - (e.g., stock exchanges, matching engines, 'dark' pools, etc.) regardless of the numerous disparate trading platforms used to submit the trades to, or the different record layouts or programming languages used at, the different trading venues. By means of the sophisticated FTEN data-mapping engine, FTEN was able to correlate each data element to its individual owner(s) as well as to each relevant financially accountable intermediary party(s). This was achievable because at the most fundamental level, electronic information all breaks down into ones and zeros.[17]

For a given trading firm (e.g., a proprietary trading group, high frequency trading (HFT) firm, hedge fund, etc.), FTEN could present their trades in real-time across all markets despite using multiple trading platforms, going through multiple financial intermediaries and ending up at 50+ disparate trading venues. For each given financial intermediary (e.g., a bank, broker, etc.),

[17] See http://www.electronics-tutorials.ws/binary/bin_1.html.

FTEN could present in real-time the trades for which they were financially accountable. By means of the FTEN data-mapping engine, FTEN could 'slice and dice' trading data to show firms their dynamic, aggregated real-time risk exposure thereby enabling real time transparency and risk management control.

Initially, there was some push back because the FTEN invention (referred to as "RiskXposure" or "RX"[18]) highlighted what was actually going on during the trading day. Prior to this time, in certain circumstances a trading firm could trade millions (even billions) of dollars more than they had been authorized – so long as they unwound their positions before the end of the day and returned to their authorized financial position – no one would be the wiser. However, financially accountable intermediaries had factored the "looseness" of systems into the credit and other arrangements that they granted to trading firms. Now that they could actually see their dynamic, aggregated real-time risk exposure, the risk to financial intermediaries was substantially reduced and they were more willing to extend increased credit to qualified trading firms. By making risk management quantifiable, financially accountable intermediaries were able to better align their risk and reward so everybody won.

Before being acquired by NASDA OMX in 2010, FTEN was the largest processor of real-time financial securities risk management in the world – each trading day providing real-time risk management and surveillance for up to 17 billion executed shares of U.S. equities, accounting for $150 billion in risk calculations.[19] After being acquired by NASDAQ OMX, FTEN risk management technology was offered to domestic and international clients, NASDAQ 's own domestic trading venues and the 70+ exchanges powered by NASDAQ OMX technology around the globe.

As NASDAQ OMX executives, the founders of Anonos next developed a big data partnership with Amazon Web Services (AWS) to enable electronic storage of financial books and records via cloud computing (i.e., "in the cloud") in a manner that satisfied strict regulatory requirements that financial data cannot be altered or deleted. This well-received cloud-based big data approach to financial books and records made significant cost reductions possible while at the same time enabling significant improvements in functionality.[20]

[18] "RiskXposure" and "RX" are trademarks of FTEN, Inc. owned by NASDAQ OMX.
[19] See http://ir.nasdaqomx.com/releasedetail.cfm?ReleaseID=537252.
[20] See Nasdaq OMX launches financial services cloud with Amazon Web Services at http://www.bankingtech.com/49065/nasdaq-omx-launches-financial-services-cloud-with-amazon-web-services/; Nasdaq OMX Sets up Data Storage Solution in the Amazon Cloud at http://www.referencedatareview.com/blog/nasdaq-omx-sets-data-storage-solution-amazon-cloud; Nasdaq, Amazon Launch Data Management Platform at http://www.waterstechnology.com/sell-side-technology/news/2208160/nasdaq-and-amazon-launch-data-management-platform; AWS Case Study: NASDAQ OMX FinQloud at http://aws.amazon.com/solutions/case-studies/nasdaq-finqloud/; NASDAQ OMX FinQloud - A Cloud Solution for the Financial Services Industry at http://aws.amazon.com/blogs/aws/nasdaq-finqloud/; NASDAQ OMX Launches FinQloud Powered by Amazon Web Services (AWS) at http://ir.nasdaqomx.com/releasedetail.cfm?ReleaseID=709164; Nasdaq OMX FinQloud R3 Meets SEC/CFTC Regulatory Requirements at http://www.wallstreetandtech.com/data-management/nasdaq-omx-finqloud-r3-meets-sec-cftc-regulatory-requirements-say-consultants/d/d-id/1268024

Risk Management by Dynamically Disassociating Associated Data Elements – the Data Privacy Industry

The consumer Internet industry generally claims that it needs real-time transparency to support current economic models – many vendors claim they need to know "who" a user is at all times in order to support a free Internet.[21] The Anonos founders challenged themselves to come up with a revolutionary "leap-frog" improvement from the sophisticated data mapping engine approach they successfully implemented in the financial markets to apply to the consumer Internet. They set out to see if they could develop a new and novel platform that would enable monetization in roughly the same manner as done today – *if not better.* Their hypothesis was that vendors would not need to know "who" a user is if they could tell "what" the user wanted – their belief was that vendors chase "who" users are in an effort to try to figure out "what" users may desire to purchase. But vendors are sometimes more incorrect than correct and can offend users by delivering inappropriate ads or delivering appropriate ads long after the demand for an advertised product or service is satisfied.

They began working with engineers; "white hat hackers" and trusted advisors to refine and improve upon their goal of bringing sophisticated risk management methodologies to the consumer Internet. But when they began talking with global data privacy professionals from "*Fortune* 50" corporations, they were told, "If you have what it looks like you have – you have no idea what you have." The view of certain data privacy professionals was that Anonos had invented a novel, unique and innovative application of technology that was larger than the consumer Internet industry with potential domestic and international applications in numerous areas including healthcare, consumer finance, intelligence and other data driven industries.

Anonos Two-Step Dynamic Anonymity - minimizing the risk of re-identification to the point that it is so remote that it represents an acceptable mathematically quantifiable risk of identifying an individual.

> ***Step 1***: Dynamic De-Identifiers or DDIDs are associated with a data subject on a dynamic basis - changing dynamically based on selected time, purpose, location-based and / or other criteria. DDIDs are then re-assigned to different data subjects at different times for different purposes making it impracticable to accurately track or profile DDIDs external to the system.
>
> ***Step 2***: - Internal to the system, information pertaining to different DDIDs used at different times for different data subjects for different purposes together with information concerning the activity of the data subjects that occurred when associated with specific DDIDs is stored in a secure database referred to as the Anonos Circle of

[21] See http://www.usnews.com/opinion/articles/2011/01/03/do-not-track-rules-would-put-a-stop-to-the-internet-as-we-know-it

Trust or "CoT." This information is retained for future use as approved by the data subject / trusted parties / proxies by accessing "keys" that bear no relationship or association to the underlying data but which provide access to applicable information by accessing a data mapping engine which correlates the dynamically assigned and re-assignable DDIDs to data subjects, information and activity.

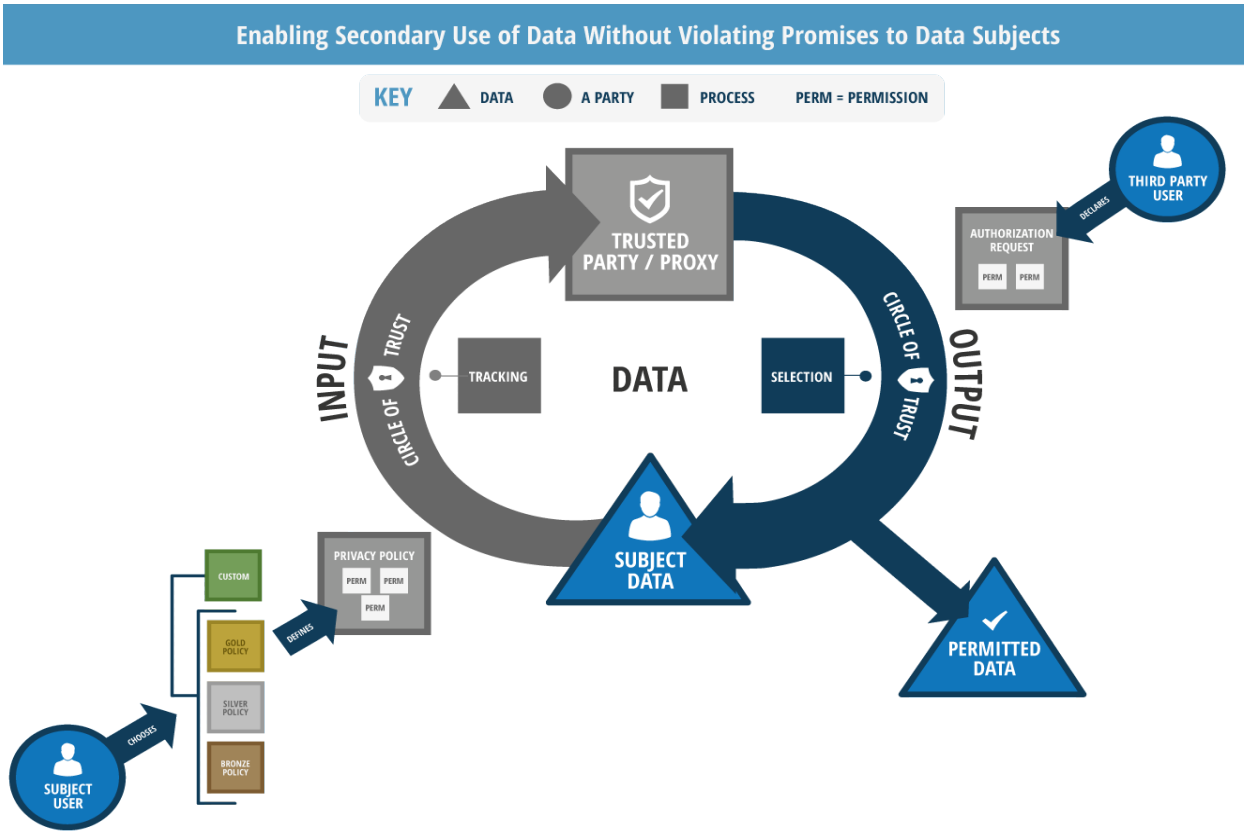
In the context of the consumer Internet, this would be comparable to every time a user visits a website, they were viewed as a first-time user with a new "cookie" or other identifier assigned to them. When the user was done with a browsing session, their cache, cookies and history could be stored within a secure Circle of Trust (CoT) enabling the user to retain the benefit of information associated with their browsing activity. When the user wanted a website to know who they were, they could identify themselves to the website - but prior to that time - *they would remain dynamically anonymous.*

Tracking information gathered during each browsing session, possibly augmented with information from the CoT representing "what" the user is interested in without revealing "who" they are, could be used to support delivery of targeted advertising. And, when a user was ready to engage in a transaction, identifying information could be accessed from the CoT as necessary to consummate the transaction. If adopted on a widespread basis, this approach could even become the default so users could be served ads based on "what" they are interested in without having to reveal "who" they are. Additionally, users could "opt-out" to receive only generic ads (such as would be the case in a true Do Not Track environment) or alternatively "opt-in" by sharing even more personalized qualifying characteristics from the CoT in order to receive even more targeted / personalized ads – *all without revealing their identity* by means of dynamically assigned and re-assignable Dynamic De-Identifiers (DDIDs) *thereby overcoming the shortcomings of static anonymity* highlighted in the answer to Question 11 (including corresponding footnotes 10 through 13) on page 6 above.

One potential application in the context of the consumer Internet relates to the interaction of a user with a hypothetical travel website. Some travel websites appear to increase the cost shown to a user for a ticket when the user checks back on the price of the ticket. This increase may not reflect an increase in the cost of the ticket generally, but rather, an increase in price for a particular user based on their apparent interest in the ticket.[22] Anonos two-step dynamic anonymity (referred to as "Dynamic Anonymity") would enable users to be treated in a nondiscriminatory basis in this example. A user would always be viewed as a "first time" visitor to a website – thereby always seeing the same price shown to other parties visiting the site – until such time as they were prepared to make a purchase at which point identifying information could be accessed from the CoT as necessary to consummate the transaction.

[22] See http://www.usatoday.com/story/travel/columnist/mcgee/2013/04/03/do-travel-deals-change-based-on-your-browsing-history/2021993/

The ***Anonos Circle of Trust (CoT)*** manages data use by "Users" in accordance with permissions (PERMS) managed by trusted parties / proxies.



"Users" may be the data subjects themselves who are the subject of the data in question (e.g., users, consumers, patients, etc. with respect to their own data – for purposes hereof, "Subject Users"); and / or third parties who are not the subject of the data in question (e.g., vendors, merchants, healthcare providers, etc. – for purposes hereof, "Third Party Users").

PERMs relate to allowable operations such as what data can be used by whom, for what purpose, what time period, etc. PERMS may also specify desired anonymization levels such as when / where / how to use Dynamic De-Identifiers (DDIDs) in the context of providing anonymity for the identity and / or activities of a data subject, when to use other privacy-enhancing techniques in connection with, or in lieu of, DDIDs, when to provide identifying information to facilitate transactions, etc.

In Data Subject implementations of Anonos, Subject Users establish customized PERMS for use of their data by means of pre-set policies (e.g., Gold / Silver / Bronze) that translate into fine-

grained dynamic permissions or alternatively may select a “Custom” option to specify more detailed dynamic parameters.

In Stewardship implementations of Anonos, Third Party Users establish PERMs that enable data use / access in compliance with applicable corporate, legislative and / or regulatory data use / privacy requirements.

In healthcare, DDIDs could help facilitate self-regulation to improve longitudinal studies since DDIDs change over time and information associated with new DDIDs can reflect new and additional information without revealing the identity of a patient. This could be accomplished by using DDIDs to separate “context” or “meta” from the data necessary to perform analysis. The results of the analysis could be shared with a Trusted Party / Proxy who would apply the “context” or “meta” to the data resulting from the analysis.

There are a multitude of players in the healthcare industry – many of which use different data structures. The Anonos Dynamic Anonymity risk management approach could support collection of disparate data from different sources in different formats, normalize the information into a common structure and separate “context” or “meta” from “content” by means of dynamically assigning, reassigning and tracking DDIDs to enable effective research and analysis without revealing identifying information. This methodology could allow the linking of data together about a single person from disparate sources without having to worry about getting consent because individuals would not be identifiable as a result of the process. Only within the CoT would identifying information be accessible by means of access to the mapping engine that correlates information to individuals.

With appropriate oversight and regulation, Trusted Parties / Proxies could offer controls via a Circle of Trust (CoT) to help reconcile tensions between identifiable and functional information. For example, currently in healthcare / life science research, significant “data minimization” efforts are undertaken to ensure that only the minimal amount of identifiable information is used in research because of potential risk to individuals of re-identification. If methodologies such as the Anonos CoT are proven to effectively eliminate the risk to individuals, much of the burden placed on regulators regarding enforcement of laws and the burden on companies associated with privacy reviews and engineering could be substantially reduced. At the same time, more complete data sets could be made available for healthcare-related research and development.